State of the Practice of Software Anti-Tamper

Capt David Chaboya
Air Force Research Labs
Anti-Tamper and Software Protection Initiative (AT-SPI) Technology Office

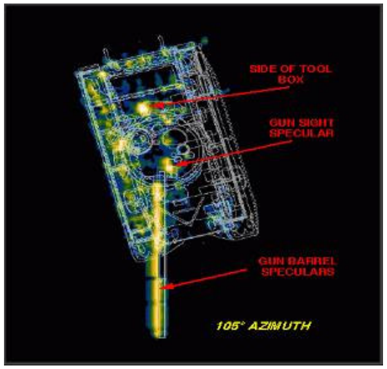
20 Jun 2007

Introduction

- AT-SPI Background
- Understanding the RE Threat
- Software Protection Techniques
- Protection Case Studies
- Software Protection Vendors
- Conclusion

Software Protection Initiative (SPI)

- Goal: Protect critical DoD application software (running on general purpose computers) from piracy and exploitation
- Lead: DUSD(S&T)
  - **Office of Primary Responsibility (OPR): AFRL AT-SPI Technology Office**



Scientific & Engineering/Modeling & Simulation Software

Mission Support Software

Enterprise Software containing critical personnel, pay, or medical information

Mission

Anti-Tamper Software Protection Office

- To deter the reverse engineering (RE) and exploitation of our military’s critical technology…..

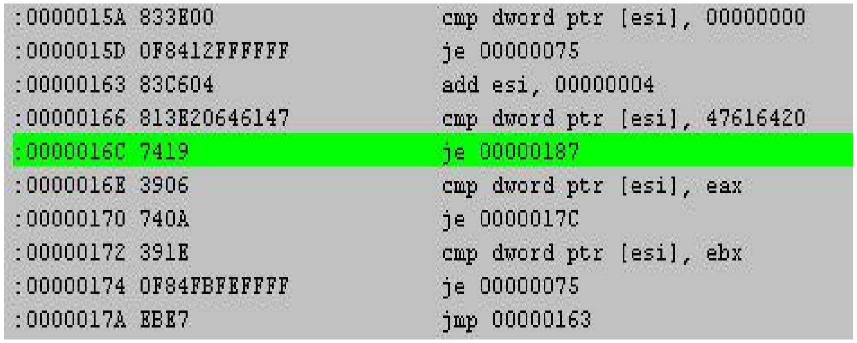
- AC130U
  – ~609,000 source lines of code (SLOC)
- F-22
  – ~2 million SLOC
- JSF
  – ~19 million SLOC

```
_VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include
#endif
#include "resource.h"
// CDMotionApp:
// See DMotion.cpp for the
//
class CDMotionApp : public
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard
        //{{AFX_VIRTUAL(
        public:
        virtual BOOL
        //}}AFX_VIRTUAL

// Implementation
        //{{AFX_MSG(
        afx_msg void
                // NOTE -
                //    DO NOT
                MSG
```

Cutting the pilot out of the locked cockpit of an F-22.

Reverse Engineering



```
:0000015A 833E00            cmp dword ptr [esi], 00000000
:0000015D 0F8412FFFFFF      je 00000075
:00000163 83C604            add esi, 00000004
:00000166 813E20646147      cmp dword ptr [esi], 47616420
:0000016C 7419              je 00000187
:0000016E 3906              cmp dword ptr [esi], eax
:00000170 740A              je 0000017C
:00000172 391E              cmp dword ptr [esi], ebx
:00000174 0F84FBFEFFFF      je 00000075
:0000017A EBE7              jmp 00000163
```

$$TMF = \left\{ \frac{\int_0^5 f^3 A(f)\,df}{\int_0^5 A(f)\,df} \right\}^{\frac{1}{3}}$$

Intellectual Property

Commercial Piracy

- Business Software Alliance (BSA) – 2006 Global Software Piracy Study
  - 35% of software installed worldwide illegal
  - $34 billion in pirated software
- Commercial companies seek to limit initial piracy/reverse engineering

coverstory By Nicholas Cravotta, Technical Editor

Prying eyes

THE GREATEST DOOR LOCK IN THE WORLD IS INEFFECTIVE IF YOU LEAVE THE KEY UNDER THE MAT. WITH CRYPTOGRAPHIC KEYS SO STRONG, WHY BREAK THEM WHEN THEY'RE SO MUCH EASIER TO STEAL?

Illustration by Mike O'Leary

Commercial Piracy

Consumer Education

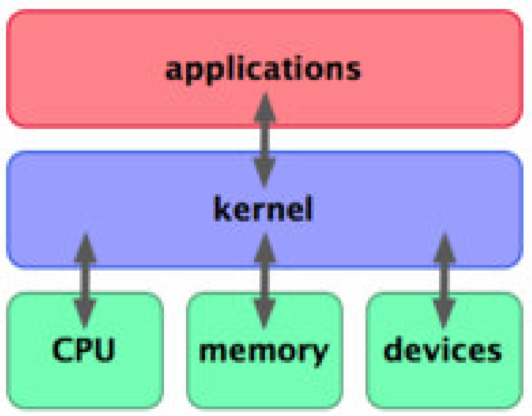
Garret the Ferret

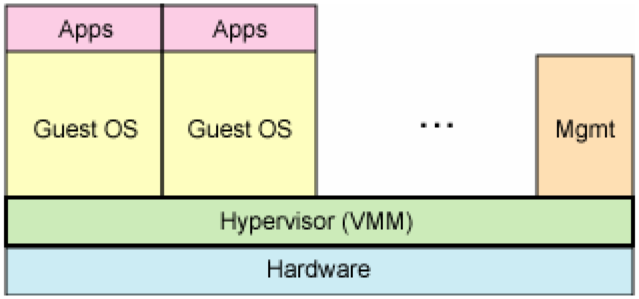
-Copyright Crusader

Source: http://www.playitcybersafe.com/pdfs/Curriculum-CC-2005.pdf

RE Threat

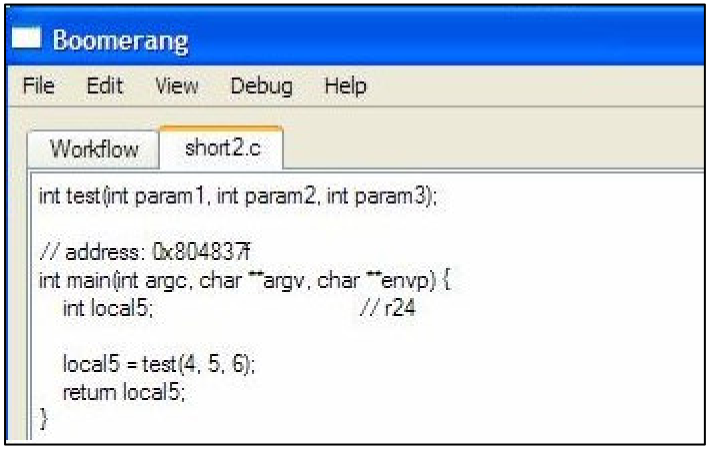
- Access
- Analysis
- Understanding





Tools of the Trade
Static Analysis

- Decompilers
  - Boomerang
  - IDAPro beta plugin

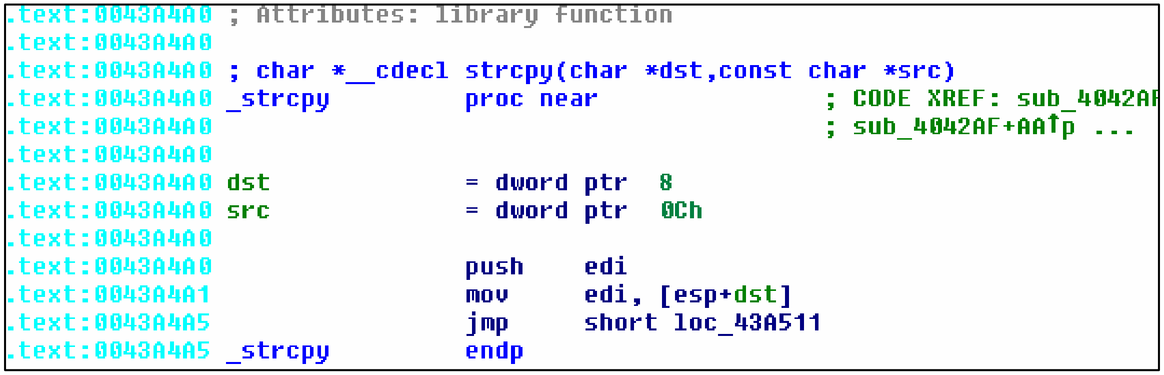


```
int test(int param1, int param2, int param3);

// address: 0x804837f
int main(int argc, char **argv, char **envp) {
    int local5;                         // r24

    local5 = test(4, 5, 6);
    return local5;
}
```

- Disassemblers
  - IDAPro

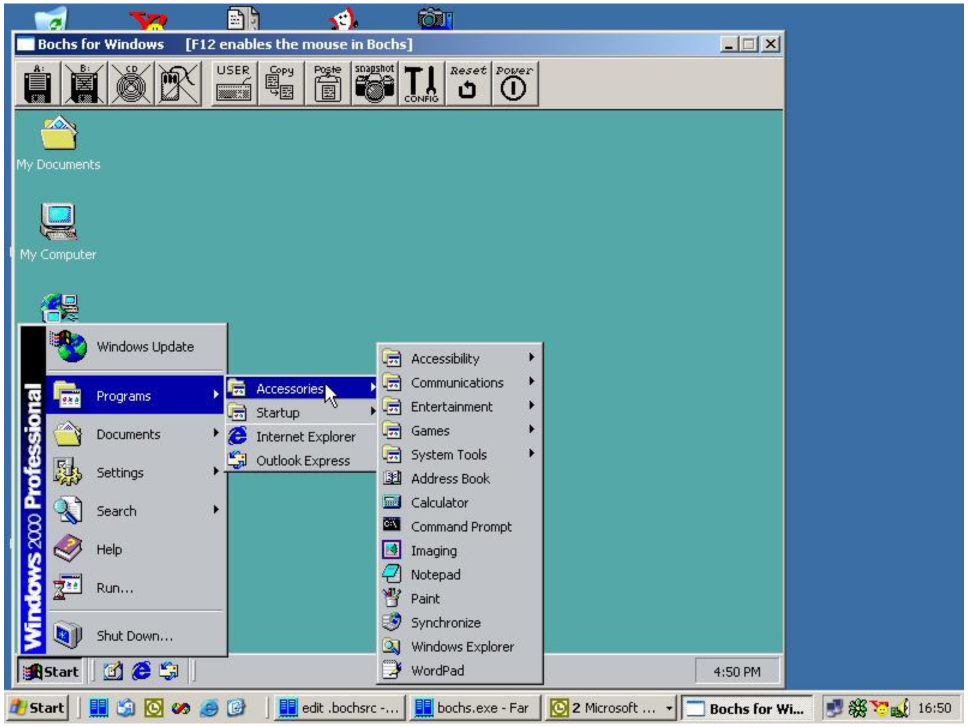


```
.text:0043A4A0 ; Attributes: library function
.text:0043A4A0
.text:0043A4A0 ; char *__cdecl strcpy(char *dst,const char *src)
.text:0043A4A0 _strcpy         proc near               ; CODE XREF: sub_4042AF
.text:0043A4A0                                         ; sub_4042AF+AA↑p ...
.text:0043A4A0
.text:0043A4A0 dst             = dword ptr  8
.text:0043A4A0 src             = dword ptr  0Ch
.text:0043A4A0
.text:0043A4A0                 push    edi
.text:0043A4A1                 mov     edi, [esp+dst]
.text:0043A4A5                 jmp     short loc_43A511
.text:0043A4A5 _strcpy         endp
```

Tools of the Trade
Dynamic Analysis

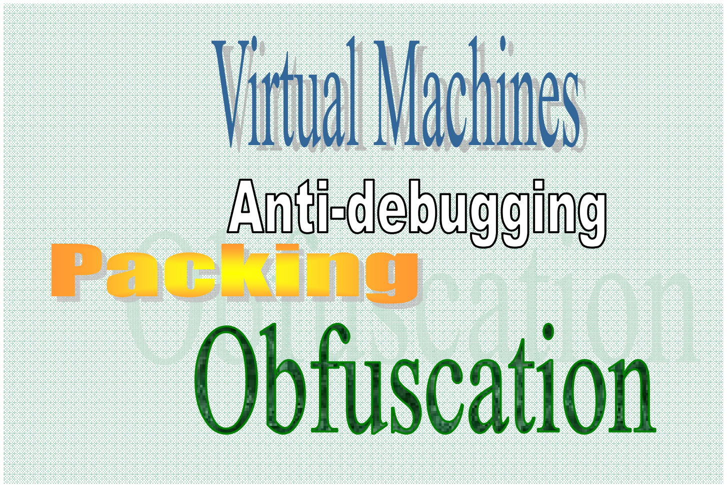
- Debuggers
  - Ollydbg
  - WinDbg
  - VAMPiRE
  - Hardware ICE

- Emulators
  - Bochs
  - Custom Virtualizers



Software Protection Techniques

- Hardware Storage/Processing
- Obfuscation
- Anti-debugging
- Encryption
- Checksums
- Diversity

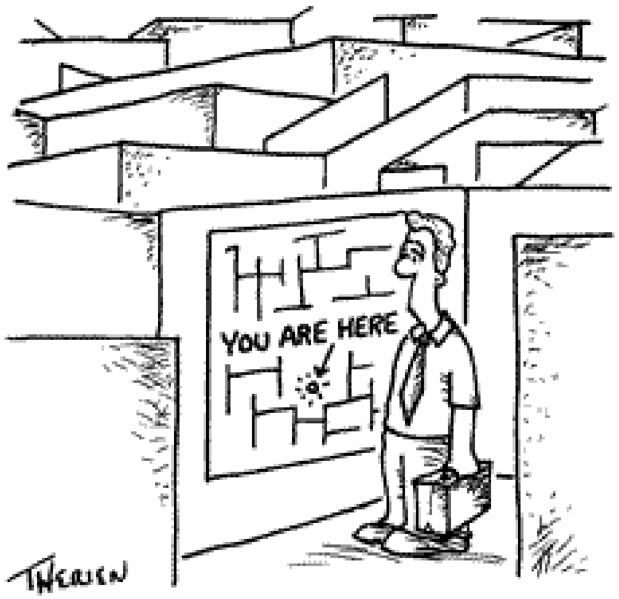


Software Anti-Tamper (AT)

- Two major types in industry
  - Encryption wrappers
  - Integrated protections

WHO IS IT?
SLANE

Source: http://www.slane.co.nz/cartoons.html



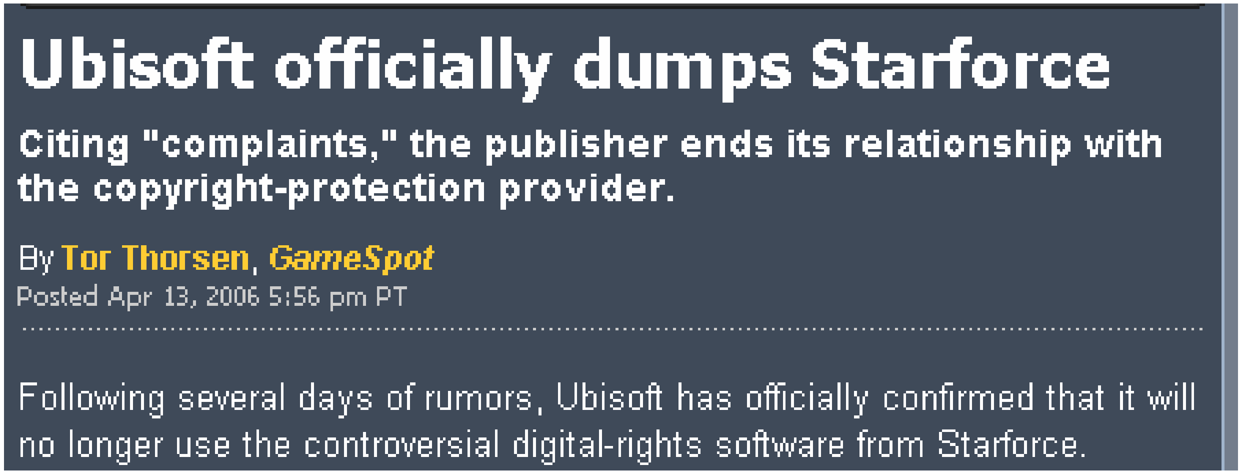
Source: www.6seconds.org/anabel/map.html

Protections: Why they Fail

- Causes problems for the end user
- Negatively impacts performance
- Opens security holes
- Tedious to apply
- Easily broken
  - BORE attacks

Starforce
Case Study

- $5 Million dollar lawsuit claiming software DRM was insecure
- Users claimed StarForce causes computer instability and crashes



Ubisoft officially dumps Starforce

Citing "complaints," the publisher ends its relationship with the copyright-protection provider.

By Tor Thorsen, *GameSpot*
Posted Apr 13, 2006 5:56 pm PT

Following several days of rumors, Ubisoft has officially confirmed that it will no longer use the controversial digital-rights software from Starforce.

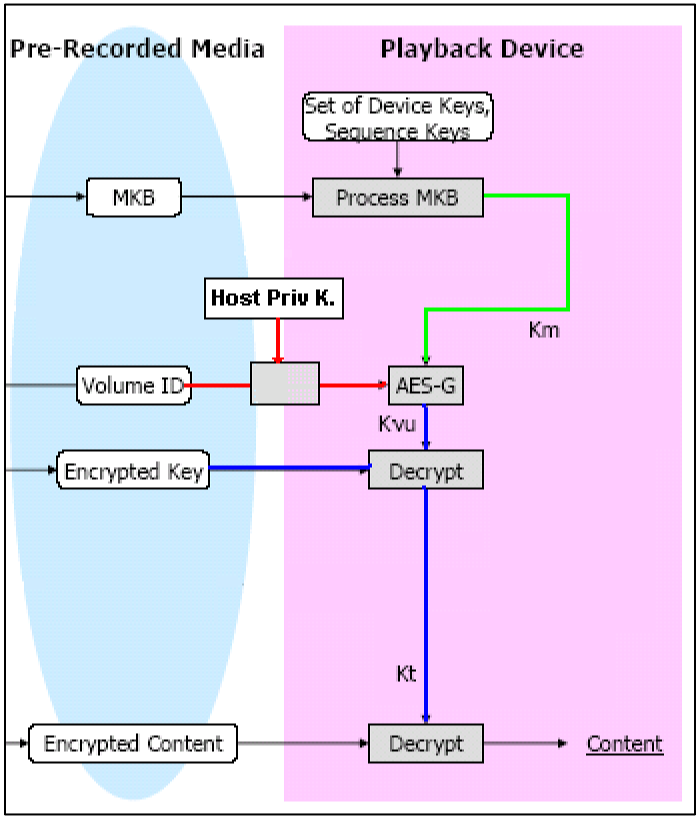
Source: http://www.gamespot.com/news/6147655.html

Sony XCP
Case Study

- Sony BMG music CDs shipped with copy protection scheme
- Protection installs system driver that hides any file or process that begins with $sys$
- Protection device driver left system open to privilege escalation attack

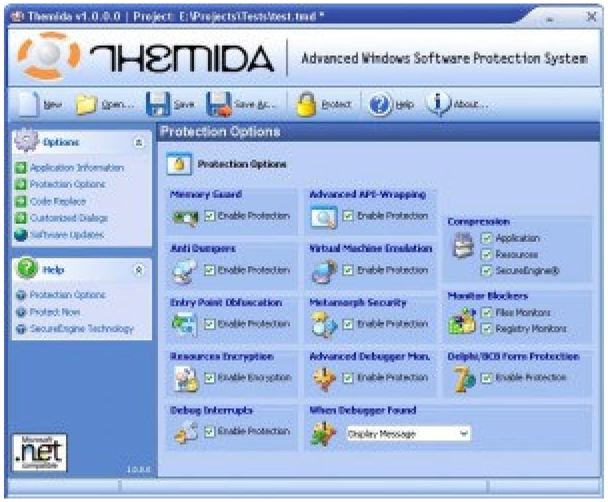
AACS
Case Study

- Advanced Access Content System
  - Copy protection
  - Modification/Decryption protection
  - Renewability and revocation
- Encryption only protects data at rest
  - Code (e.g., keys) visible upon execution



XProtector
Case Study

- Software protection focused on kernel mode driver
- Discontinued due to repeated published breaks
- Updated product renamed as Themida
- Protection transitioned from kernel module to Virtual Machine



Protection Options

Memory Guard ☑ Enable Protection

Advanced API-Wrapping ☑ Enable Protection

Compression ☑ Application ☑ Resources ☑ SecureEngine®

Anti Dumpers ☑ Enable Protection

Virtual Machine Emulation ☑ Enable Protection

Entry Point Obfuscation ☑ Enable Protection

Metamorph Security ☑ Enable Protection

Monitor Blockers ☑ Files Monitors ☑ Registry Monitors

Resources Encryption ☑ Enable Encryption

Advanced Debugger Mon. ☑ Enable Protection

Delphi/BCB Form Protection ☑ Enable Protection

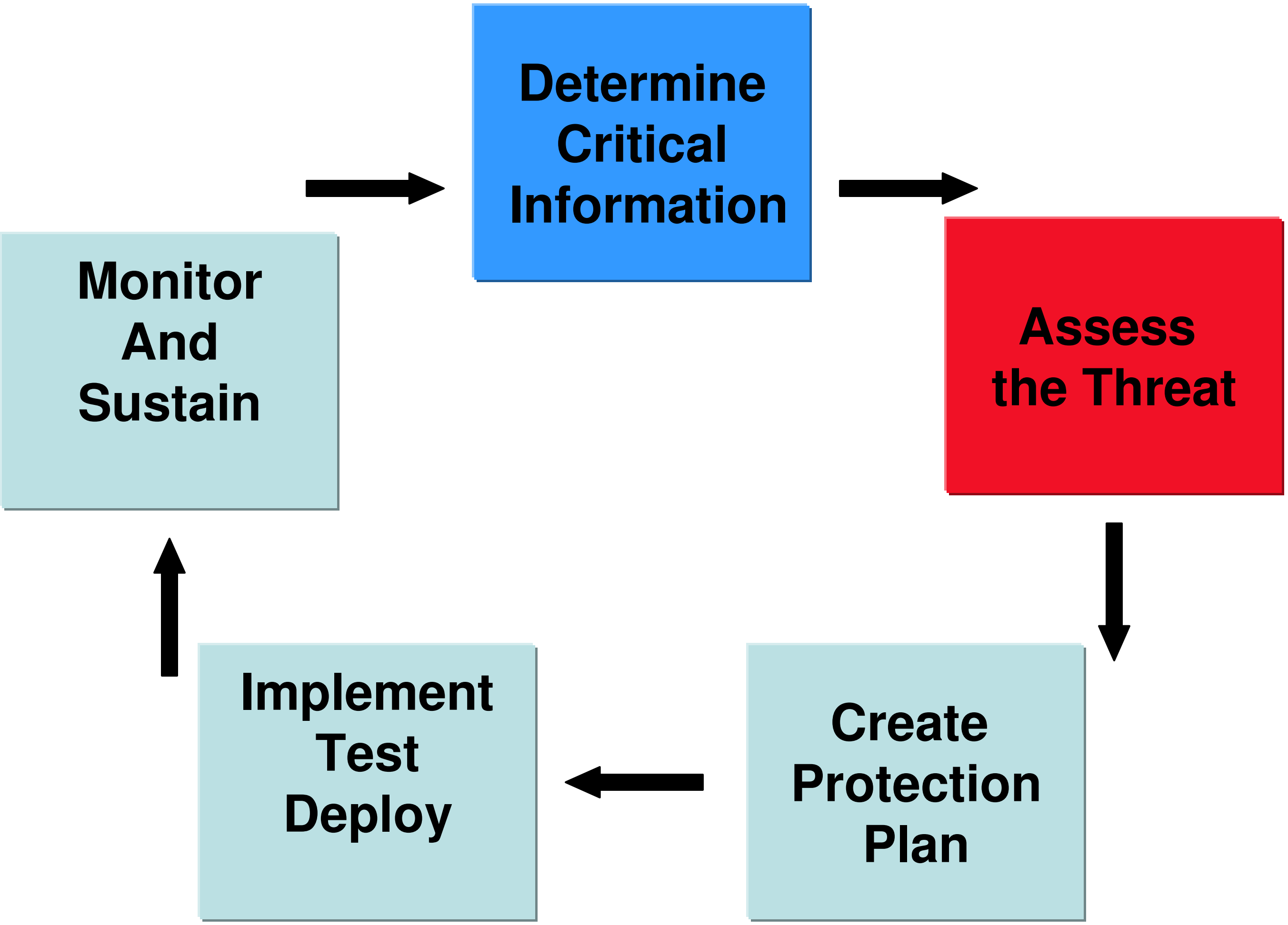
Debug Interrupts ☑ Enable Protection

When Debugger Found: Display Message

Ideal Software Protection

- High level of security against best attackers
- Low performance impact
- Resistant to repeat/automated attacks
- Protects against all forms of runtime analysis
- Securely locks to hardware
- Easy to apply

Protection Process



Metrics

- Difficult questions
  - How much protection is enough?
  - How long will it last?
- Determining metrics
  - Blackhat assessments
  - Red teams
  - Markets
  - Formal modeling

Sample of Protection Vendors

- Arxan
  - http://www.arxan.com/solutions.html

- Pikewerks
  - http://www.pikewerks.com/research.htm

- Cloakware
  - http://www.cloakware.com/products_services/security_suite/

- Luna
  - http://www.lunainnovations.com/research/secure.htm

Conclusion

- Software Protection (AT) is still very much in its infancy
- Significant research into formalizing protection techniques and assessment metrics
- Autonomous and dynamic/polymorphic protections will improve and become more prevalent
- Increased support from hardware (e.g., TPM) and software (e.g., Microsoft) vendors for secure systems

Questions?

Capt David Chaboya
Air Force Research Labs
Anti-Tamper and Software Protection
Initiative (AT-SPI) Technology Office
Email: david.chaboya@wpafb.af.mil
Phone: 937-320-9068

Acronyms

- AACS - Advanced Access Content System
- AFRL – Air Force Research Labs
- AT – Anti Tamper
- BORE – Break Once Run Everywhere
- DRM – Digital Rights Management
- DUSD(S&T) – Deputy Undersecretary of Defense (Science and Technology)
- OPR – Office of Primary Responsibility
- RE – Reverse Engineering
- SLOC – Source Lines of Code
- SPI – Software Protection Initiative
- TPM – Trusted Platform Module